## CLAIM AMENDMENTS

This listing of claims will replace all prior versions and listings of claims in the application.

1. (Currently Amended) A processor ~~for encrypting and decrypting~~ that performs an encryption/decryption operation ~~data~~, the processor comprising:

a control device that receives ~~a data word for encryption or decryption~~ at least one initial key, the control device comprising:

a memory that temporarily stores ~~an~~ the at least one initial key, and

at least one external key input that receives the at least one initial key from a source;

a round key generator connected to the control device via at least one ~~further~~ communication device, wherein the round key generator receives the ~~data word~~ at least one initial key from the control device ~~for calculating~~ to calculate at least one round key and transfers the at least one round key to the memory of the control device; ~~and~~

at least one encryption/decryption device comprising:

at least one external data input that receives external data,

an input that receives the at least one round key from the memory of the control device, and

at least one external data output that outputs data processed with the at least one round key, wherein the at least one encryption/decryption device and the round key generator communicate solely via the control device, and the control device transmits intermediate results to the round key generator to perform recursive calculation of the at least one round key;

a first request line that sends requests from the at least one encryption/decryption device to the control device; and

a second request line that sends requests from the round key generator to the control device, wherein the at least one encryption/decryption device and the round key generator both transmit requests on the respective first and second request lines to start the encryption/decryption operation after both requests are met.

2. (Currently Amended) The processor of claim 1, wherein the at least one communication device further comprises:

~~first and second request lines;~~

first and second release lines; and

first and second data lines.

3. (Previously Presented) The processor of claim 2, wherein the first and second request lines, the first and second release lines, and the first and second data lines at least partially use a single physical path.

4. (Previously Presented) The processor of claim 1, wherein the at least one round key is temporarily stored in the memory of the control device.

5. (Previously Presented) The processor of claim 1, wherein the at least one round key is accessed using a rotating pointer.

6. (Previously Presented) The processor of claim 1, wherein the communication between the control device and the at least one encryption/decryption device and between the control device and the round key generator is accomplished using at least one handshake protocol.

7. (Previously Presented) The processor of claim 1, wherein the operation of the control device, of the at least one encryption/decryption device, and of the round key generator are asynchronous with respect to one another.

8. (Currently Amended) The processor of claim 1, wherein the round key generator ~~is adapted to perform~~ performs a dummy operation.

9. (Previously Presented) The processor of claim 1, wherein a time between the calculating of the at least one round key by the round key generator and the processing of the external data using the at least one round key is variable.

10. (Previously Presented) The processor of claim 1, wherein the processor is an Advanced Encryption Standard (AES) coprocessor.

11. (Currently Amended) A method of ~~encrypting and/or decrypting data~~ performing an encryption/decryption operation using a processor, the method comprising:

sending a first request on a first request line from at least one encryption/decryption device to a control device and a second request on a second request line from a round key generator to the control device to start the encryption/decryption operation after both requests are met;

reading at least one initial key into ~~a~~ the control device, wherein the at least one initial key is obtained from a source other than ~~a~~ the round key generator;

reading external data into the at least one encryption/decryption device;

reading at least one data word needed to calculate at least one round key from at least one storage device of the control device;

transferring the at least one data word to the round key generator;

calculating at least one round key recursively on the basis of the at least one data word by using the round key generator;

transferring the ~~calculated~~ at least one round key to the control device; ~~and~~

storing the ~~transferred~~ at least one round key in the at least one storage device;

transferring the at least one round key from the at least one storage device to the at least one encryption/decryption device;

processing the external data by using the at least one encryption/decryption device, using the at least one round key, and ~~using~~ the processed data are made available at at least one external data output; and

repeating the method as often as necessary to encrypt or decrypt a set of external data,

wherein the control device transmits intermediate results to the round key generator to perform recursive calculation of the at least one round key.

12. (Previously Presented) The method of claim 11, wherein communication between the control device and the at least one encryption/decryption device, and

between the control device and the round key generator is accomplished using at least one handshake protocol.

13. (Previously Presented) The method of claim 11, wherein the operation of the control device, of the at least one encryption/decryption device, and of the round key generator are asynchronous with respect to one another.

14. (Previously Presented) The method of claim 11, wherein the at least one round key is accessed using a rotating pointer.

15. (Previously Presented) The method of claim 11, further comprising:

performing a dummy operation using the round key generator.

16. (Currently Amended) The method of claim 11, wherein a time between the calculating of the at least one round key by the round key generator and the processing of the external data using the at least one round key is variable.

17. (Previously Presented) The method of claim 11, wherein the processor is an Advanced Encryption Standard (AES) coprocessor.